| Envision HEALTHCARE | Ethics & Compliance Department | | |
|---|---|---|---|
| | Policy No.: 76 | **Created:** | 01/2018 |
| | | **Reviewed:** | 09/2024 |
| | | **Revised:** | |

# HIPAA: REPORTING AND INVESTIGATING SUSPECTED BREACHES

## SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

## PURPOSE:

Envision Healthcare Operating, Inc. and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Reporting and Investigating Suspected Breaches policy to ensure that standards are developed and employed for reporting and responding to an incident involving the breach of Unsecured Protected Health Information ("PHI") or a breach of Personal Information, as those terms are defined in this policy and in the HIPAA Privacy and Security rules.

## POLICY:

**Breaches of Unsecured Protected Health Information**

The Company will comply with all applicable laws and regulations to determine when the Company must notify patients that a breach of that patient's Unsecured PHI has occurred. Unsecured PHI means all information that is not encrypted according to the Company's standards, has not been shredded or has not, in some other way, been made unusable or unreadable to unauthorized individuals

A breach of Unsecured PHI is the unauthorized acquisition, access, use, or disclosure of Unsecured PHI in a manner which compromises the security or privacy of the PHI. An unauthorized access, use, or disclosure of Unsecured PHI is presumed to be a breach unless the Company can demonstrate that there is a low probability that the PHI has been compromised. The Company's Privacy Official, in conjunction with others designated by the Privacy Official, is responsible for making the determination on the probability of compromise.

A breach does not include:

(1) Any unintentional acquisition, access, or use of PHI by a member of the Company's workforce or a Company Business Associate if the acquisition, access, or use was made in good faith and would otherwise be within the scope of the workforce member's (or the Business Associate's) scope of authority as long as there is no further inappropriate use or disclosure; or

(2) Any inadvertent disclosure by a person who is authorized to access PHI at the Company to another person who is authorized to access the Company PHI provided there is no further inappropriate use or disclosure.

(3) A disclosure of PHI where the Company has a good faith belief that the unauthorized person who received the information would not reasonably be able to retain the information.

If any member of the Company's workforce discovers or suspects that there has been a breach of Unprotected PHI, he/she should report the matter to the Privacy or Security Official immediately.

The Privacy Official will investigate the report and make a determination as to whether the incident constitutes a breach of Unsecured PHI. When investigating the incident, the Privacy Official will determine whether the Company has reporting obligations to an individual or to a client. In determining whether the incident is or is not a breach of Unsecured PHI, the Privacy Official will determine whether there is a low probability that the PHI has been compromised. In making his/her determination, the Privacy Official will take into consideration:

(1) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

(2) The unauthorized person who used the PHI or to whom the disclosure was made;

(3) Whether the PHI was actually acquired or viewed; and

(4) The extent to which the risk to the PHI has been mitigated.

The Privacy Official will log all pertinent information regarding the situation.

**Notice**

If the Privacy Official determines a breach of Unsecured PHI has occurred, the Privacy Official will notify affected individuals without unreasonable delay, and no later than sixty (60) days after the discovery of the breach.

A) The Notice to Individuals will include, to the extent possible:

(1) A brief description of the breach, including the date of the breach and the date of the discovery of the breach, if known;

(2) A description of the types of information that were compromised (for example, whether the information included a full name, account number, diagnosis, or some other type of information);

(3) Information on steps the individual can take to protect him or herself from potential harm resulting in from the breach;

(4) A brief description of actions taken by the Company to investigate the breach, to mitigate harm, and to protect against any further breaches; and

(5) Contact procedures for individuals to ask questions or learn of additional information (which must include a toll-free telephone number, an email address, a website, or a postal address).

B) Notice will be sent in writing by first-class mail to the individual, or by electronic mail if the individual agrees to electronic notice.

C) If the Company has insufficient or out-of-date contact information, the Company will attempt to identify a substitute form of notice to reach the individual. If there is insufficient or out of date contact information for fewer than ten (10) individuals, then substitute notice may be provided by telephone, an alternative form of written notice, or other means. If there is insufficient or out of date contact information for more than ten (10) individuals, the substitute notice must be either:

(1) In the form of a conspicuous posting for a period of ninety (90) days on the home page of the Company's website; or

(2) A conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside.

In both cases, the notification must include a toll-free phone number that remains active for at least ninety (90) days where an individual can learn whether the individual's Unsecured PHI may be included in the breach.

D) If the case is deemed to require urgency because of the potential for misuse of the Unsecured PHI, the Privacy Official may provide information by telephone or other means in addition to the written notice above.

E) If a breach of Unsecured PHI involves more than five hundred (500) residents of a state or jurisdiction, the Privacy Official will notify prominent media outlets serving the state or jurisdiction. The media notification must be given without unreasonable delay and in all cases must be given within sixty (60) days after discovery of the breach involving more than five hundred (500) residents of a state.

F) If the breach involves Unsecured PHI of five hundred (500) or more individuals, the Privacy Official will provide notice to the Secretary of U.S. Department of Health and Human Services ("HHS") at the same time as notice is provided to the affected individuals and in the manner specified on the HHS website.

G) If the breach involves Unsecured PHI of fewer than five hundred (500) individuals, the Privacy Official will provide notice to HHS no later than sixty (60) days after the end of the calendar year in which the breach was discovered, in the manner specified on the HHS website.

H) The Privacy Official will maintain a log or other documentation of any breaches of Unsecured PHI that occur during a calendar year.

I) If a law enforcement official determines that a notification, notice, or posting otherwise required by law would impede a criminal investigation or cause damage to national security, the Company will comply with the following standards:

(1) If the statement is in writing and specifies the time for which a delay is required, the Privacy Official will delay such notification, notice, or posting for the time period specified by the law enforcement official; or

(2) If the statement is made orally, the Privacy Official will document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than thirty (30) days from the date of the oral statement, unless the law enforcement official provides a written statement as described above.

**Breaches of Personal Information**

The Company will comply with all applicable laws and regulations to determine when the Company must notify patients that a breach of that patient's PII has occurred.

A) The Company will reevaluate any applicable state law requirements if there is a breach that includes computerized personal information or PII. State law requirements will vary and often depend on the state of residence of the patient. Therefore, employees should report all suspected breaches to the Privacy Official.

B) While state law requirements vary, generally states define personal information to include a person's name in conjunction with a social security number or other identification number (such as a driver's license number) or a person's name in conjunction with an account number or credit card number in combination with a required security code or access code.

C) The Company's Privacy Official will evaluate whether the potential breach includes a breach of personal information that may require notification under applicable state laws.

## POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.